Securitoo | Anti-Virus

TOUJOURS À JOUR

Manuel d'utilisation





Manuel d'utilisation

Présentation :

Utilisation :

Questions fréquentes :

Protection en temps réel : la technologie PVD

Securitoo Anti-Virus a été conçu pour répondre aux besoins en matière de lutte contre les virus exprimés par les particuliers et les administrateurs de réseaux d'entreprises. Ainsi, pour être optimale, la fonction de détection des virus se devait d'être totalement transparente et s'exécuter en temps réel.

Le fonctionnement de Securitoo Anti-Virus repose sur la technologie PVD (Protection Virale Dynamique) qui protège votre ordinateur lorsque ce dernier fait appel à ses disques. Cette technologie assure une protection permanente lorsqu'un fichier est ouvert, copié, déplacé, renommé ou même téléchargé depuis Internet.

La protection en temps réel fonctionne de manière transparente en tâche de fond. Elle recherche la présence éventuelle de virus lorsque vous accédez à des fichiers stockés sur disquettes, disques-durs, CD-Roms ou sur lecteurs réseau sans toutefois ralentir votre ordinateur. Si vous tentez d'ouvrir un fichier infecté, la PVD interrompt automatiquement l'exécution du virus et vous permet alors de vous en débarrasser.

Remarque : Afin d'empêcher les virus dits de "secteur d'amorçage" de se propager, la protection en temps réel analyse également les disquettes à l'arrêt ou au démarrage de l'ordinateur. Si aucune disquette ne se trouve dans le lecteur à ce moment-là, ce dernier peut émettre un léger "bourdonnement". Ceci est un phénomène tout à fait normal. Il n'y a pas lieu de s'inquiéter.

Pour savoir si la protection en temps réel est active, regardez l'icône d'état de Securitoo Anti-Virus dans la barre de tâches à côté de l'horloge. Si l'icône est sur **ON**, la PVD est active. Dans le cas contraire, l'icône est sur **OFF**.



Une seconde possibilité existe pour vérifier si la PVD est active : Cliquez deux fois sur l'icône **OO** dans la barre des tâches à côté de l'horloge afin d'afficher le panneau de contrôle de Securitoo Anti-Virus, puis sur le bouton **Paramètres.**



Accès au panneau de contrôle de Securitoo Anti-Virus

Si l'état du module-application *F-Secure Anti-Virus* est "*Activé*" **(fig.1)** la protection en temps réel est active et fournit une protection continue. Si tel n'était pas le cas, nous vous renvoyons à la section, plus complète, "Comment vérifier que mon Anti-Virus est actif ?" du chapitre **"Questions fréquentes"** du manuel que vous avez entre les mains afin d'activer votre produit.

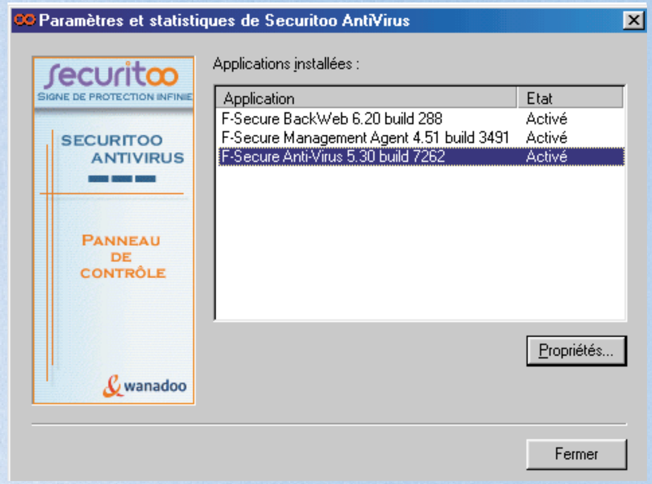


fig.1

Recherche manuelle de virus

Securitoo Anti-Virus reposant sur la technologie PVD (voir pages précédentes), il n'est pas indispensable de recourir à une analyse manuelle de fichiers ou de disques. Toutefois, vous avez la possibilité d'effectuer un "*scan*" manuel de vos fichiers et de vos disques via l'un des trois menus suivants :

- **menu contextuel**
  (cliquez avec le bouton droit de la souris sur un fichier, un dossier ou un disque).
- **menu Paramètres et Statistiques de l'icône Securitoo**
  dans la barre de tâches à côté de l'horloge.
- **menu Démarrer de Windows.**

Au cours d'une analyse, la boîte de dialogue Statistiques de l'analyse manuelle **(fig.1)** affiche un indicateur d'avancement, ainsi que des statistiques sur l'analyse en cours. Pour interrompre une analyse en cours, cliquez sur **Arrêter**. A la fin de l'analyse, un rapport est généré. Vous pouvez le visualiser en cliquant sur le bouton **Afficher le rapport**.

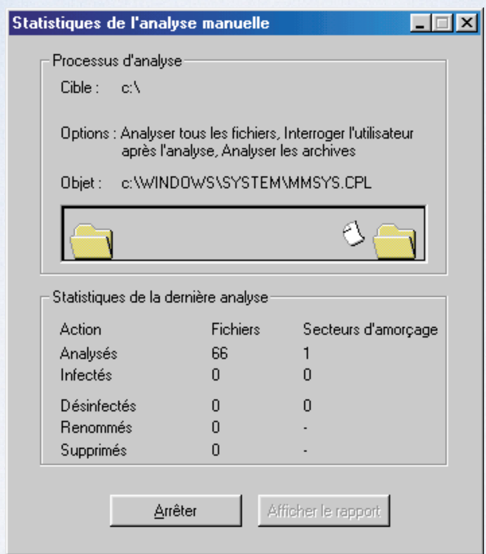


fig.1

Menu contextuel

Pour rechercher des virus dans un fichier, un dossier ou une disquette, cliquez dessus avec le bouton droit de la souris, puis sélectionnez l'option *"Rechercher des virus..."* dans le menu contextuel qui s'affichera **(fig.2)**. Tout fichier, dossier ou lecteur peut être analysé de cette manière, quelle que soit son extension.

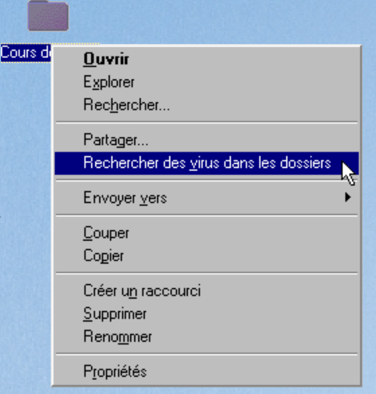
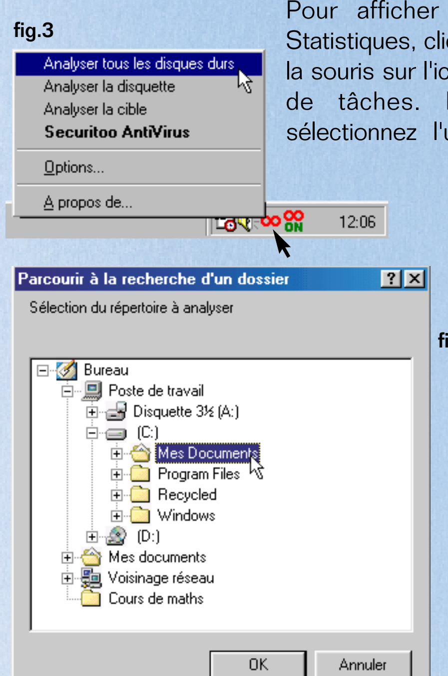


fig.2

Menu Paramètres et Statistiques de l'icône Securitoo dans la barre de tâches

fig.3



Pour afficher le menu Paramètres et Statistiques, cliquez avec le bouton droit de la souris sur l'icône **OO** **(fig.3)** dans la barre de tâches. Pour lancer un "*scan*", sélectionnez l'une des options d'analyse figurant dans le menu : Analyser tous les disques durs, Analyser la disquette ou Analyser la cible.

fig.4

Si vous sélectionnez l'option "*Analyser la cible*", vous devrez sélectionner le dossier ou le disque à analyser **(fig.4)**.

Menu Démarrer de Windows

Le groupe de programmes de Securitoo contient des raccourcis permettant d'analyser les disques durs, les disquettes et les dossiers **(fig.5)**.

Pour lancer une analyse, sélectionnez l'une des commandes d'analyse disponibles dans le menu : *Analyser tous les disques durs locaux*, *Analyser la disquette* ou *Analyser le dossier*. Si vous sélectionnez l'option *Analyser le dossier*, vous devrez sélectionner le dossier ou le disque à analyser **(fig.4)**.

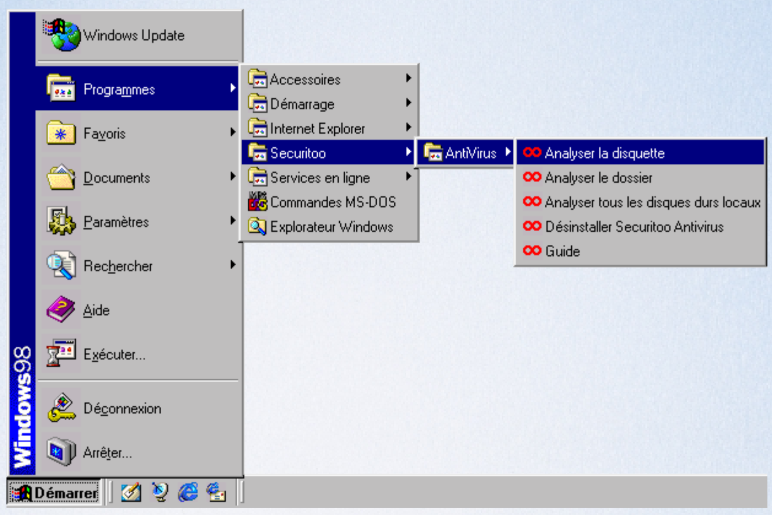


fig.5

Que faire lorsqu'un virus est détecté ?

Lorsque vous utilisez l'ordinateur et qu'un virus est détecté, Securitoo Anti-Virus stoppe immédiatement l'exécution de celui-ci et lance automatiquement l'Assistant de Nettoyage **(fig.1)** qui constitue la procédure standard d'élimination du code malveillant.

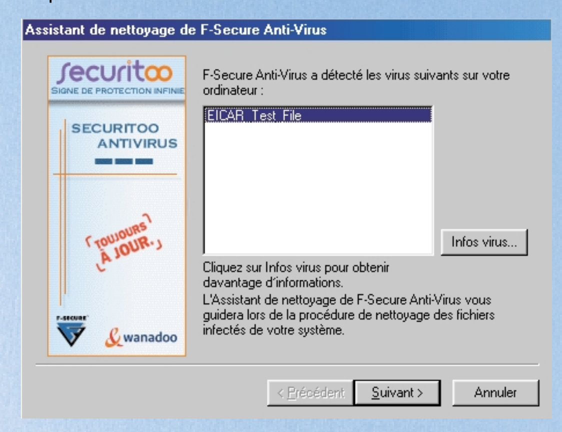


fig.1

L'Assistant de Nettoyage vous informe alors du nom du virus détecté. Pour continuer la procédure d'éradication, cliquez sur le bouton **Suivant.**

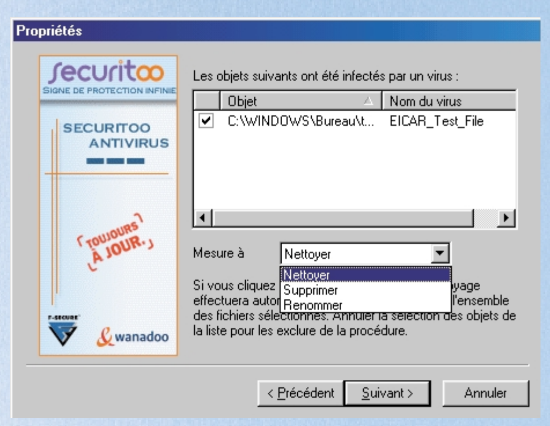


fig.2

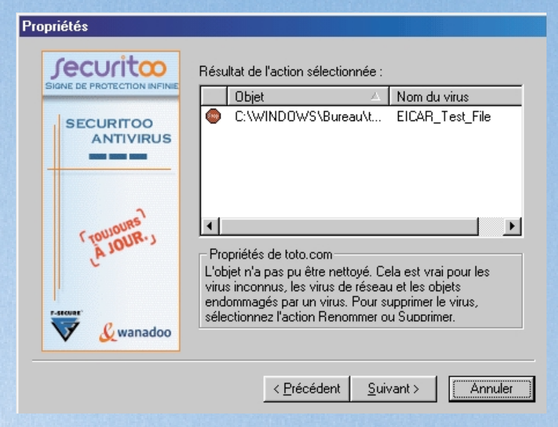
Vous pouvez à cet instant décider de l'action à mener à l'encontre du fichier infecté par le virus : le ***Nettoyer***, le ***Supprimer*** ou le ***Renommer***.

Cochez tout d'abord le nom du fichier infecté comme sur la figure 2 (p6).

Nettoyer vous permet d'ôter le virus du fichier qu'il a infecté, mais cette action dépend de la nature même du virus. En effet, certains virus suppriment un morceau du fichier qu'ils infectent. Il est alors impossible de "sauver" le fichier infecté car on ne pourra jamais lui rendre son contenu - sain - d'origine. D'autres virus s'ajoutent simplement au contenu du fichier qu'ils infectent. Il est alors possible de rendre au fichier son apparence d'origine.

Supprimer permet d'effacer purement et simplement le fichier infecté du disque sur lequel il se trouve. Cette opération est le meilleur choix si *Nettoyer* a échoué en fonction de la nature du virus (cf. ci-dessus). Toutefois, chaque médaille a son revers et choisir de supprimer un fichier de son disque peut entraîner des dysfonctionnements si ce dernier jouait un rôle clé dans le système ou l'ensemble dans lequel il était intégré. (Exemple : un virus infecte le fichier msword.exe et vous décidez de le supprimer. Ceci entraînera l'impossibilité d'utiliser Microsoft™ Word™ car il se trouve que msword.exe représente le logiciel Word™ lui-même).

Renommer permet de donner un autre nom au fichier infecté, de telle sorte qu'il ne soit plus "joignable" par le programme ou système auquel il était originellement rattaché. Toutefois, le virus subsiste en son sein. Ceci constitue donc un choix qui doit être mûrement réfléchi par l'utilisateur de l'ordinateur.



La figure 3 nous montre le résultat d'une tentative de Nettoyage qui n'a pu fonctionner.

fig.3

Dans ce cas, cliquez sur le bouton **Précédent**, puis cochez comme vous l'avez déjà fait le nom du fichier infecté **(fig.2)**. Choisissez alors une autre action à mener, comme par exemple *Supprimer* ou *Renommer*. Dans le cas d'un succès, la figure 3 bis s'affichera.



fig.3 bis

Cliquez alors sur le bouton **Suivant**.

Si l'analyse a été déclenchée de manière manuelle, l'Assistant de Nettoyage vous proposera d'éditer un rapport sur l'action menée **(fig.4)**.

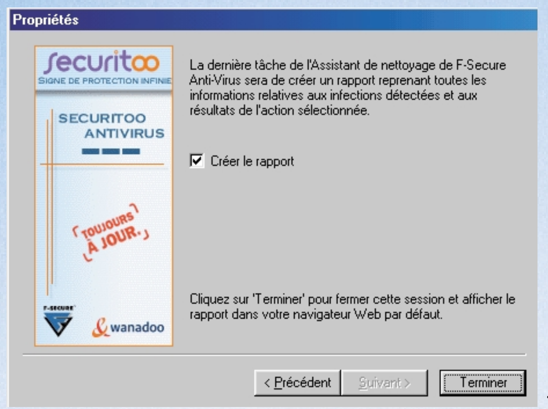


fig.4

Il ne vous reste plus qu'à cliquer sur le bouton **Terminer** pour clore l'Assistant de Nettoyage.

Panneau de contrôle de Securitoo Anti-Virus

Le panneau de contrôle de Securitoo Anti-Virus vous permet d'effectuer toutes les vérifications relatives à l'état des modules, au mode de fonctionnement de ceux-ci ainsi qu'aux mises à jour des fichiers de signatures virales.

Vous pouvez y accéder en double-cliquant sur l'icône Securitoo dans la barre de tâches à côté de l'horloge :

La fenêtre illustrée en figure 1 s'affichera alors :

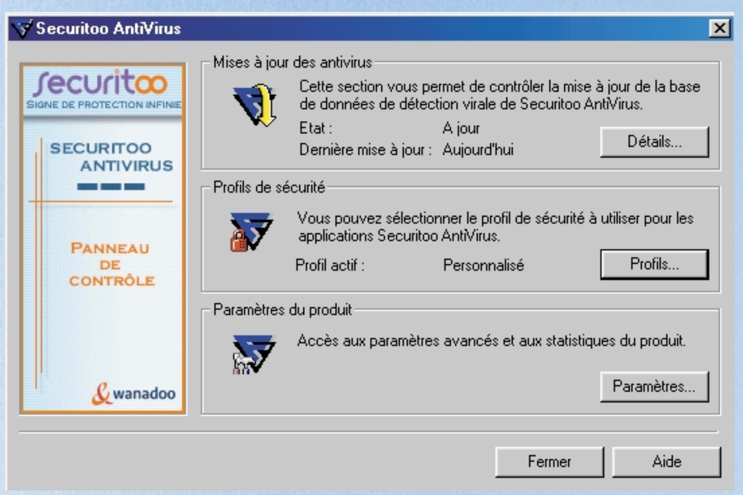


fig.1

Le bouton **Détails** de l'encart *Mises à jour des Anti-Virus* vous donnera des renseignements à propos de la dernière mise à jour effectuée.

Le bouton **Profils** de l'encart *Profils de sécurité* vous permet de définir le niveau de protection de Securitoo Anti-Virus en sélectionnant l'un des **trois profils pré-établis** : "***Normal***" (niveau de protection optimisé pour une utilisation quotidienne), "***Personnalisé***" (profil identique au précédent mais qui vous permet de modifier certains paramètres de la protection anti-virus), et "***Paranoïde***" (surveillance en temps réel de TOUS les fichiers, y compris les archives). Nous vous conseillons cependant de ne pas utiliser ce dernier profil, surdimensionné par rapport à la menace réelle que représentent les virus et extrêmement gourmand en ressources système.Votre PC en serait extrêmement ralenti.

Le bouton **Paramètres** de l'encart *Paramètres du produit* vous permettra d'accéder au paramétrage de Securitoo Anti-Virus. C'est lui qui nous intéresse ici tout particulièrement.

En cliquant sur celui-ci, vous accédez à la fenêtre illustrée par la figure 2:

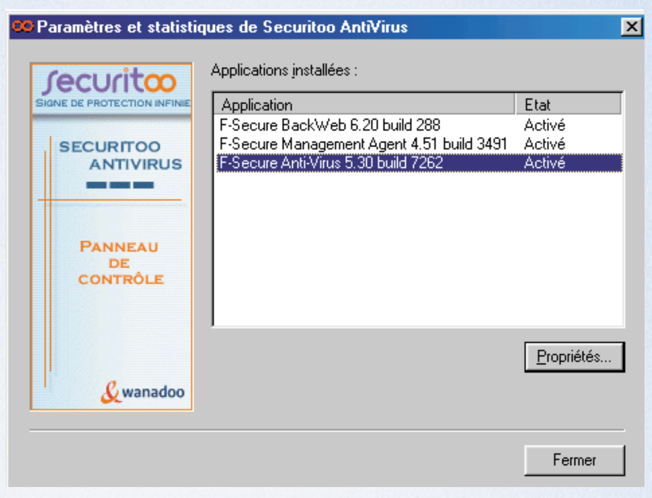


fig.2

Sélectionnez l'application F-Secure Anti-Virus et cliquez sur le bouton **Propriétés.**

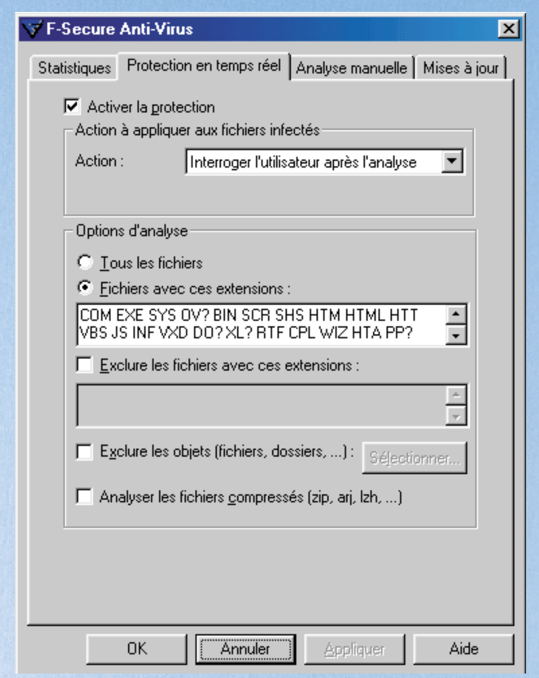


fig.3

L'onglet Protection en temps réel **(fig.3)** vous permet de régler les paramètres et le comportement de la protection en temps réel (voir la section relative à la PVD).

Activer la protection : vous pouvez choisir de désactiver la protection en temps réel, mais nous ne saurions que trop vous recommander de ne jamais le faire !!! Vous ne seriez alors pas plus protégé que si vous n'aviez justement pas d'Anti-Virus...

Action à appliquer : en cas de découverte d'un foyer d'infection viral, vous pouvez ici définir le comportement de la PVD. Elle peut :

• Interroger l'utilisateur de l'ordinateur sur l'action à mener.
C'est le choix défini par défaut.

• Tenter immédiatement un nettoyage du fichier infecté.
Toutefois, comme nous l'avons vu, cette action peut échouer en fonction de la nature du virus.
(voir la section "Que faire lorsqu'un virus est détecté ?")

• Renommer automatiquement le fichier infecté.
C'est un choix qui n'éradique pas le virus, mais qui permet de retirer le fichier de l'ensemble ou du système dans lequel il se trouvait.
(voir la section "Que faire lorsqu'un virus est détecté ?")

• Supprimer le fichier infecté.
C'est un choix judicieux car le virus ne peut résister à cette action, mais qui peut en revanche entraîner des perturbations si le fichier jouait un rôle clé au sein de l'ordinateur.
(voir la section "Que faire lorsqu'un virus est détecté ?")

• Créer uniquement un rapport.
Cette solution n'a qu'un intérêt informatif et ne doit être utilisée que lors de tests effectués par des administrateurs de réseaux d'entreprise par exemple.

Options d'analyse : Vous pouvez ici décider d'analyser tout fichier ou seulement ceux dont l'extension fait partie de la liste. Nous vous recommandons de ne pas pointer "*tous les fichiers*". En effet, nous nous trouvons dans l'onglet relatif à la Protection Virale Dynamique (PVD) dite communément Protection en Temps Réel. Si vous pointez "*tous les fichiers*", alors chaque fichier accédé sera analysé, ce qui en temps réel risque de ralentir **plus que fortement votre ordinateur.** Préférez de loin laisser le choix sur "*Fichiers avec ces extensions*". Pour la même raison, nous vous recommandons de laisser décochée la case "*Analyser les fichiers compressés*" car ceux-ci devraient être décompressés, puis ensuite analysés...

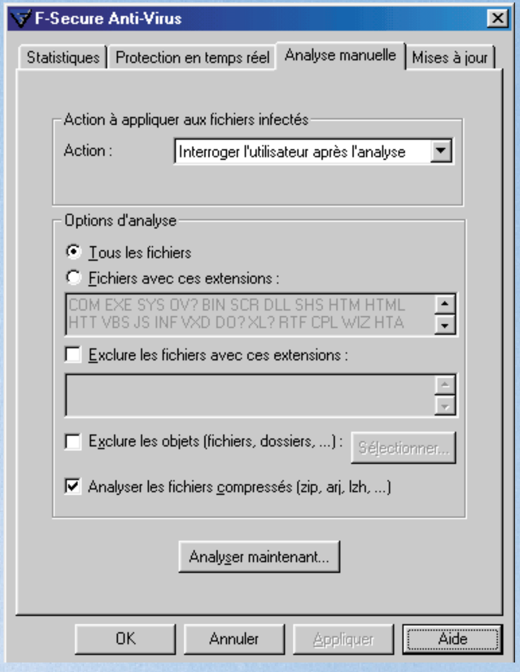


fig.4

L'onglet *Analyse manuelle* **(fig.4)** vous permet d'accéder aux mêmes paramètres, à une différence près en ce qui concerne les fichiers compressés. En mode manuel, le temps n'a forcément pas la même valeur.

En revenant sur la fenêtre illustrée par la figure 2, vous pourrez sélectionner l'application F-Secure BackWeb pour accéder à ses propriétés.

L'onglet *Etat du canal* **(fig.5)** vous permet de vérifier si une mise à jour est en cours de téléchargement et de lancer une connexion vers notre serveur de manière à - éventuellement - en recevoir une en cliquant sur le bouton **Connexion immédiate.**

F-Secure BackWeb
Etat du canal | Fichiers reçus | Paramètres
Nom du canal : Canal Securitoo
Adresse du canal : maj.securitoo.com
Etat courant : Ready
Dernière connexion 05/11/2001 17:05:04 Aucune nouveauté disponible
Connexion suivante 05/11/2001 17:06:04
Connexion immédiate
Afficher le fichier journal...
OK Annuler Appliquer

fig.5

L'onglet *Paramètres* ne doit en aucun cas être modifié **sous peine de ne plus recevoir correctement les mises à jour de votre Anti-Virus.**

Comment saisir ma clé d'enregistrement ?

NB : cette manipulation est également valable pour les personnes qui ont saisi une clé erronée et qui souhaitent corriger leur erreur.

Pour que les manipulations suivantes puissent porter leurs fruits votre connexion Internet devra être lancée !

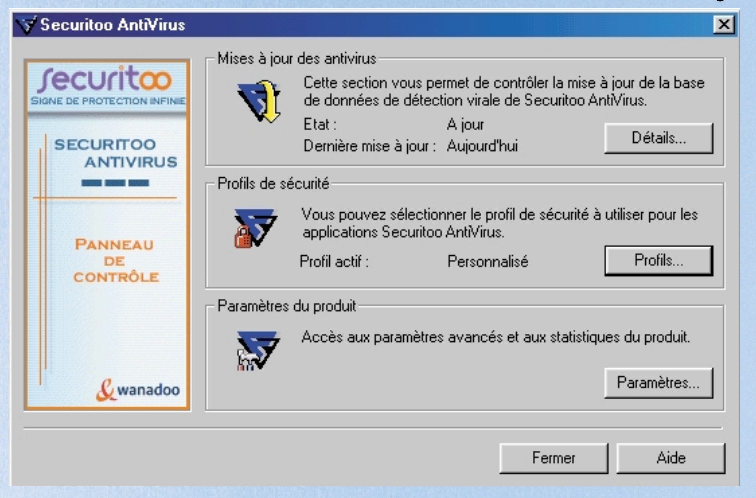
Securitoo Anti-Virus ne vous protégera réellement et complètement qu'à une seule condition : avoir saisi sa clé d'enregistrement. C'est grâce à elle que Securitoo Anti-Virus sera activé sur votre PC et que les mises à jour pourront être réalisées.

Vous pouvez accéder à cette saisie en double-cliquant sur l'icône Securitoo dans la barre de tâches à côté de l'horloge :



La fenêtre illustrée en figure 1 s'affichera alors.

fig.1



Cliquez sur le bouton **Paramètres**, vous accédez à la fenêtre illustrée par la figure 2 .

Sélectionnez l'application F-Secure BackWeb et cliquez sur le bouton **Propriétés**.

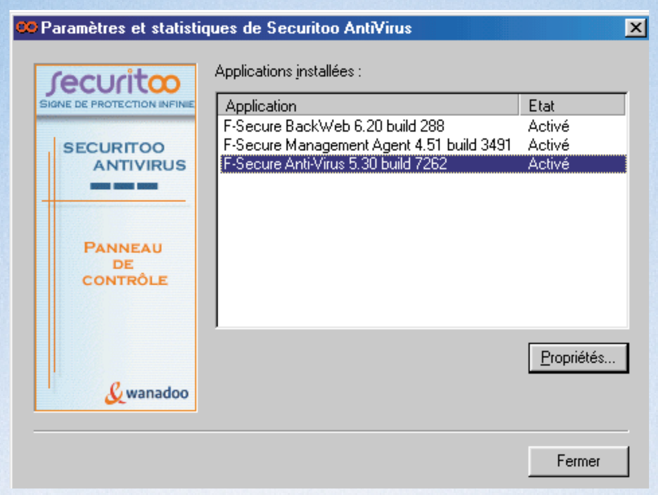


fig.2

L'onglet Paramètres **(fig.3)** vous permet d'accéder au bouton **ID utilisateur** (en bas à gauche). Cliquez sur ce bouton,

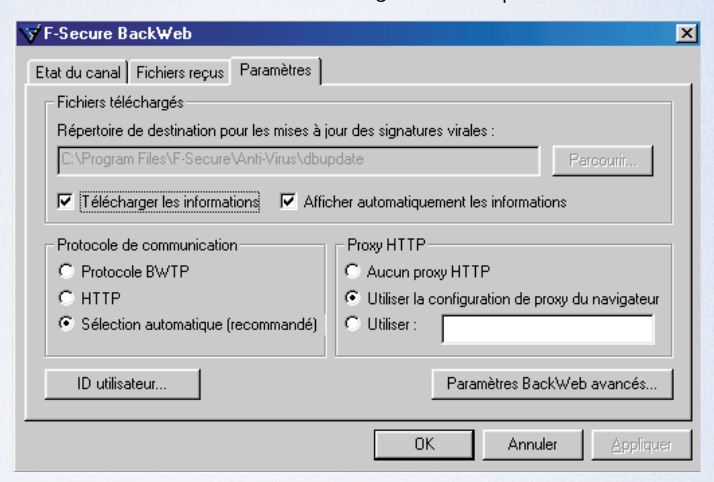


fig.3

la fenêtre illustrée par la figure 4 s'ouvrira. Il vous suffira d'y inscrire votre clé d'enregistrement, de valider par un appui sur le bouton **OK**, puis de refermer l'une après l'autre les fenêtres restées ouvertes.

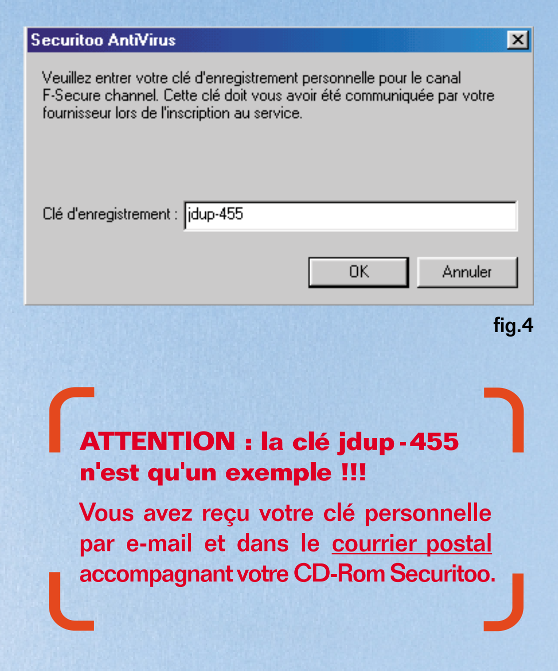


fig.4

ATTENTION : la clé jdup-455 n'est qu'un exemple !!!

Vous avez reçu votre clé personnelle par e-mail et dans le courrier postal accompagnant votre CD-Rom Securitoo.

Pensez par la suite à vérifier que votre Anti-Virus est actif. A cet effet, n'hésitez pas à visiter la section :
"Comment vérifier que mon Anti-Virus est actif ?" (p.19).

Comment vérifier que mon Anti-Virus est actif et qu'il me protège ?

Comme nous l'avons déjà vu dans la rubrique "Protection en temps réel", un indicateur visuel placé près de l'horloge de Windows vous permet de vérifier si votre Anti-Virus est actif ou pas. :



Dans le cas où la protection ne serait pas active et afin d'en connaître la raison, double-cliquez sur l'icône Securitoo dans la barre de tâches :



La fenêtre illustrée en figure 1 s'affichera alors :

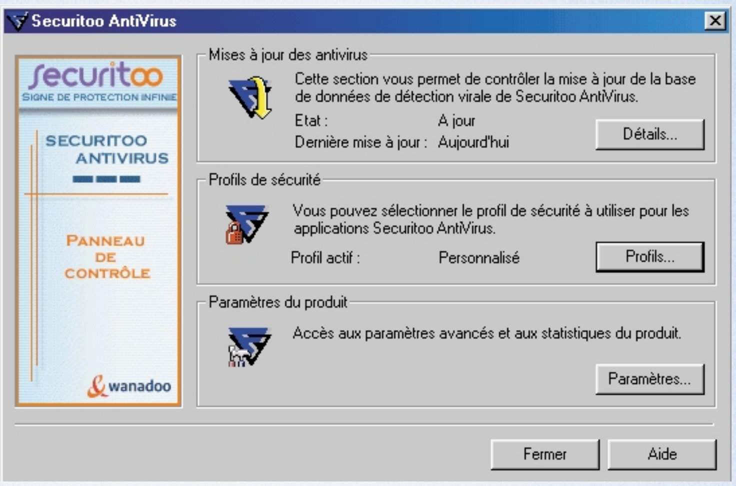


fig.1

Cliquez sur le bouton **Paramètres**, vous accédez à la fenêtre illustrée par la figure 2 :

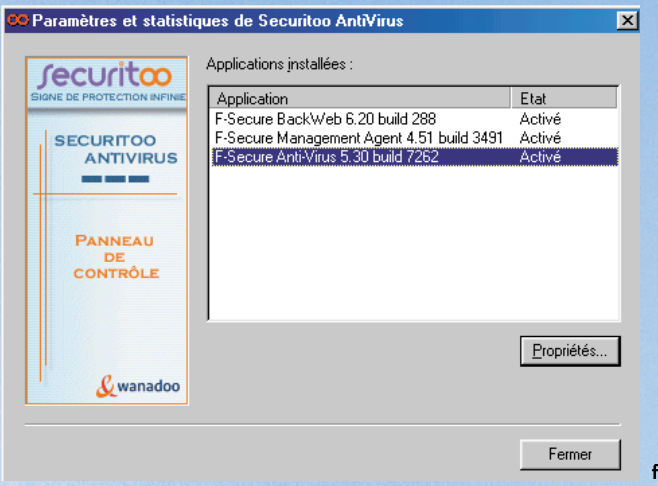


fig.2

Sélectionnez l'application *F-Secure Anti-Virus* et cliquez sur le bouton **Propriétés**.

Deux cas peuvent alors se présenter à vous : soit vous avez désactivé votre Anti-Virus manuellement (voir **fig.3** page suivante), soit ce dernier n'est pas encore activable (parce que la clé d'enregistrement saisie précédemment n'a pas encore été validée) - **(fig.3 bis)**.

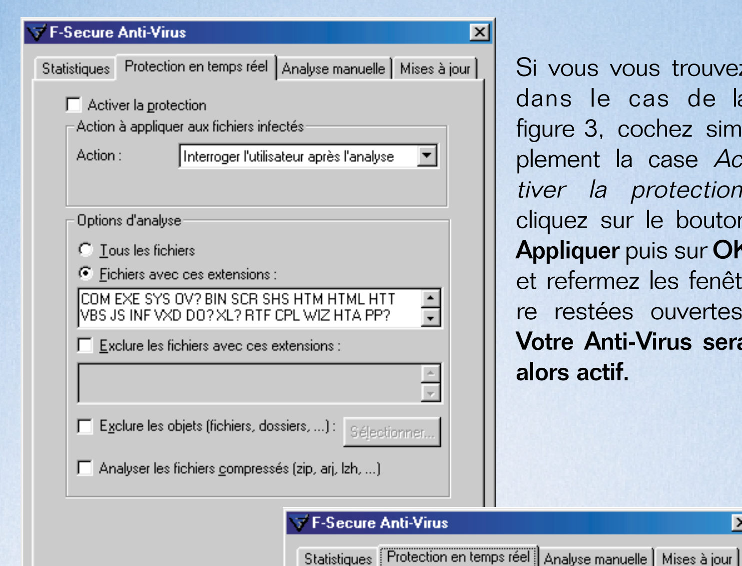


fig.3

Si vous vous trouvez dans le cas de la figure 3, cochez simplement la case *Activer la protection*, cliquez sur le bouton **Appliquer** puis sur **OK** et refermez les fenêtre restées ouvertes. **Votre Anti-Virus sera alors actif.**

Si en revanche vous êtes dans le cas de la figure 3bis, cliquez sur le bouton **OK** et suivez les indications en page 22.

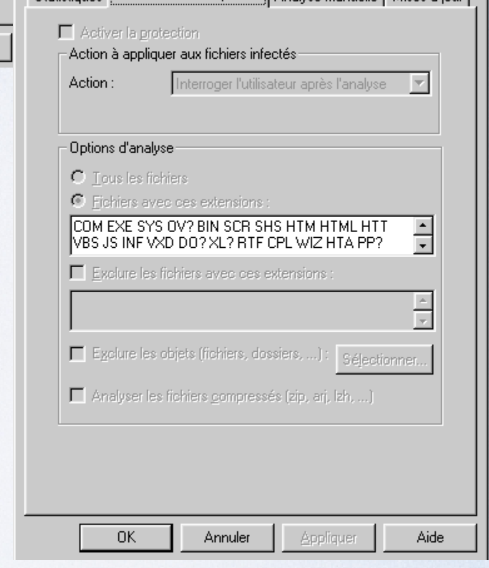


fig.3 bis

1) Sur la fenêtre représentée à la figure 2, sélectionnez *F-Secure BackWeb* et appuyez sur le bouton **Propriétés**. Vérifiez votre clé d'enregistrement comme déjà vu précédemment dans la section 'Comment saisir ma clé d'enregistrement ?" (Votre connexion Internet doit bien entendu être lancée !!!).

2) Une fois la clé vérifiée, cliquez sur l'onglet *Etat du canal*. Cliquez alors plusieurs fois à quelques dizaines de secondes d'intervalle sur le bouton **Connexion Immédiate**. La ligne "*Etat courant*" doit passer de "*Connecting to server*" à "*Ready*" et la ligne "*Dernière connexion*" doit être différente de "*Aucune nouveauté disponible*" **(fig.4)**.

F-Secure BackWeb

Etat du canal | Fichiers reçus | Paramètres

Nom du canal :	Canal Securitoo
Adresse du canal :	maj.securitoo.com
Etat courant :	Ready
Dernière connexion	05/11/2001 17:05:04 Aucune nouveauté disponible
Connexion suivante	05/11/2001 17:06:04

Connexion immédiate | Afficher le fichier journal...

OK | Annuler | Appliquer

fig.4

Attention : Si la phrase "*Aucune nouveauté disponible*" perdure, prenez contact avec notre service d'assistance technique en expliquant au technicien que vous aurez en ligne que vous venez d'effectuer les opérations décrites ci-dessus.

Comment - temporairement - désactiver mon Anti-Virus ?

Certains logiciels demandent lors de leur installation ou de leur utilisation de désactiver les programmes Anti-Virus installés sur le PC.

Nous vous renvoyons à la figure 3 de la section "Panneau de contrôle de Securitoo Anti-Virus". Vous pourrez y décocher la case "Activer la protection" afin de désactiver votre Anti-Virus.

N'oubliez pas de le réactiver après vos opérations !!!

Comment réinstaller Securitoo Anti-virus après avoir formaté mon disque dur ou changé de PC ?

La procédure de réinstallation est identique à la procédure décrite dans le “Guide d’installation”. Toutefois, il convient de contacter notre service technique par téléphone afin de procéder à une réactivation de votre clé d'enregistrement.

Dans le cas contraire votre Anti-Virus, une fois installé, ne s'activerait pas.



Configuration minimale requise :

- Processeur Pentium II - 300Mhz
- Windows 95/98/Me/XP /NT4/2000 pro
- 64 Mo de mémoire vive (RAM)
- 40 Mo d’espace disponible sur disque dur
- Connexion Internet.

Configuration standard requise* :

- Processeur Pentium II - 400Mhz
- Windows 95/98/Me/XP /NT4/2000 pro
- 128 Mo de mémoire vive (RAM)
- 40 Mo d’espace disponible sur disque dur
- Connexion Internet.

*pour un meilleur confort d’utilisation

www.securitoo.com



